REMARKS/ARGUMENTS

35 USC § 101 Rejections

The Examiner asserts that claims 1-5, 12, 17, 25, and 27-28 are not patentable because "the claimed invention as a whole fails to accomplish a practical/useful application or directed to a program per se product." This grounds for rejection is respectfully traversed.

Paragraph 0003 sets out a problem in the prior art in connection with the certification of encryption keys where there is a hierarchy of trusted authorities which must be dealt with. The present invention is directed to methods, apparatuses and computer program products which address the issue set forth in paragraph 0003. A mode of carrying out the invention is described in detail in the specification. It is submitted that addressing the problem in the prior art noted in paragraph 0003 is certainly useful in the computer arts. A practical solution is disclosed. The assertion that the disclosed invention is neither practical or useful is incorrect and therefore the rejection based on this assertion is without merit. Kindly withdraw the assertion and the rejection.

The Examiner also asserts that the (or perhaps some of the) rejected claims are directed to "a program per se product". This rejection is apparently aimed at claims 27 and 28 alone. Those two claims have been amended to recite that the computer program product is "stored on computer readable media" which should overcome this portion of the rejection.

35 USC § 102 Rejections

The Examiner rejects claims 1-17, 19- 25 and 27-28 under 35 USC § 102 as being allegedly fully anticipated by Gentry (US Publication No. 2003/0182554). This grounds for rejection is respectfully traversed.

Gentry is a pertinent reference with some similarities to the present claims but also significant differences.

Before going into the differences in detail, it should be noted that the Examiner has referenced passages from Gentry relating to the Figure 1 embodiment. In fact, this embodiment appears to be a generalized statement of the two embodiments shown in Figures 4 and 5 of Gentry. Note that in paragraph 0024 of Gentry which relates to the Figure 1 embodiment, reference is made to:

"a first intermediate shared secret component that is determined using a "first random secret and a system parameter" (see step 104)

and to

"a second intermediate shared secret component that is determined using a "second random secret and a system parameter" (see step 110)

Details of the make-up of the intermediate shared secret components are not clearly given in respect of the Figure 1 embodiment, but are provided in greater detail with relation to the embodiments of Figures 4 and 5. The differences between Gentry and the the present claims can, in fact, be more easily understood by looking at a specific example of Gentry and the comments below addressing the Figure 5 embodiment which is apparently closer to the present claims than is the embodiment of Figure 4 of Gentry.

Similar to the present invention, Gentry is based on the use of pairings (Weil or Tate).

Gentry discloses a Private Key Generator (PKG) that has a secret **s** which it uses to supply two entities A and B with respective secrets $\mathbf{S_A}$ (= $\mathbf{sP_A}$), $\mathbf{S_B}$ (= $\mathbf{sP_B}$) where $\mathbf{P_A}$ and $\mathbf{P_B}$ are public elements formed from the identities of the entities A and B respectively – see paragraph 0022 of Gentry.

The two entities A and B can now, without more ado, form a **non-interactive shared secret** S_{AB} by using bilinear mapping as is explained at line 14 of paragraph 0022 of Gentry.

The entities A and B also form an **interactive shared secret** by the exchange of intermediate shared secret components. Thus for the Figure 5 embodiment, entity A which has a secret **a**, passes **aP** to entity B, whereas entity B, which has a secret **b**, passes **bP** to entity A; **P** is a public element. Both entities can now form **abP**. This is described in paragraph 0033 of Gentry.

The entities now go on to form a common symmetric key using at least the interactive shared secret. The formation of the symmetric key seems to be the purpose of the Gentry arrangement, the symmetric key being used to secure communication between the entities.

Differences between Gentry and Claim 1

The first obvious difference is that the Gentry disclosure is concerned with generating a symmetric key for use between two entities whereas the invention, as set out in claim 1, concerns the provision to a third party by a second party of a set of verification parameters to enable the third party to verify the existence of an association between the second party and a first party. So the rejection under 35 USC § 102 is not proper as Gentry does not teach each and every limitation of claim 1.

The Examiner did not focus on this difference because the Examiner seems to be seeking to equate the values computed by one entity as the "verification parameters" of claim 1 and therefore looks more at that limitation regarding the "verification parameters". However, the Examiner is not permitted to ignore the limitations of claim 1 when rejecting it on prior art grounds.

Moreover, if one considers the nature of the verification parameters specified in claim 1, it will become apparent that they differ from the values exchanged between the entities A and B of Gentry. In fact it is only necessary to observe that according to claim 1, each of the THREE verification parameters that are output is the product of a secret held by the second party and a respective further quantity:

> "the second-party computer entity ..... computes first, second and third verification parameters as the product of a second secret with said shared secret, the second element and the first element respectively"

It should be noted that the values, which are computed, are outputted "for use by the third party" (and possibly also made publicly available). As such any value that is computed and kept secret by an entity cannot be a verification parameter of amended claim 1.

Considering values outputted and/or made publicly available by entity A of the Gentry Figure 5 embodiment (we could equally take entity B as entities A and B carry out equivalent operations):

- entity A has a public element **P_A** (strictly this is not disclosed as available from entity A but arguably this is implicit);
- entity A passes the quantity **aP** to entity B as an "intermediate shared secret component" where **a** is a secret of entity A and **P** is a public element;
- entity A may seek to prove to entity B that entity A knows the non-interactive shared secret by "generating a MAC for the first intermediate shared secret component aP using the non-interactive shared secret as the key and communicating this first MAC to the second entity" (see [0034]).

Thus, the first entity A of Gentry can be said to make available three values to the second entity B. **But these three values do not all contain a common factor that is a secret of the first entity A as is required by claim 1.** For although the intermediate shared secret component **aP** has the secret **a** as a factor, this secret of entity A does not appear as a factor in either **P_A** (formed as a hash of A's identity) or the MAC.

So in addition to failing to meet the limitations regarding the third party, Gentry also fails to anticipate the limitations regarding the first, second, and third verification parameters as recited by claim 1.

It is therefore clear that claim 1 is patentable over Gentry. Note that the above argument can be applied to all of the embodiments described in Gentry.

Claims 12, 19, 25 and 27

The same argument applies to the independent apparatus claim 19 and independent computer program product claim 27 both of which are similarly worded to claim 1 in terms of these differentiating features. The argument also applies to independent claim 12 which expresses the invention in different language but also requires a second party to generate and output three values ("first, second, and third cryptographic parameters") which have a common factor that is a private key of the second party.

Furthermore, a similar argument also applies to claim 25 (hierarchy of trusted authorities) as each non-root trusted authorities have two public parameters which have a secret of the trusted authority as a common factor (see last sub-paragraph) - in Gentry no two of the values passed by the entity A has a secret of the entity A as a common factor.

Differences between Gentry and Claim 8

Claim 8 concerns the operations carried out by the third party (or rather a third-party computer entity) in using the verification parameters to verify the existence of an association between the first and second parties. Note that the make-up of the verification parameters is not specified in claim 8 (the third party has no knowledge of this) and so the argument used above in respect of claim 1 does not apply to claim 8.

However, claim 8 specifies the carrying out of first and second checks each taking the form of a comparison of two different bilinear mappings – the bilinear mapping function is indicated in claim 8 by use of the symbol $\mathfrak{p}$, this symbol having been introduced at line 8, page 2 of the specification as:

"a computable bilinear map $\mathfrak{p}$, for example, a Tate pairing t or Weil pairing $\hat{e}$"

In Gentry each entity A and B uses a bilinear map to form the non-interactive shared secret S_{AB} – see Gentry's paragraph 0022. This is apparently the only described use of bilinear mappings in Gentry. There is no disclosure of any check involving the comparison of two different bilinear mappings. The closest Gentry comes is in the process mentioned above in which entity A may seek to prove to entity B that entity A knows the non-interactive shared secret S_{AB} by "generating a MAC for the first intermediate shared secret component using the non-interactive shared secret as the key and communicating this first MAC to the second entity" (see Gentry's paragraph 0034) - on receiving the MAC value the second entity B can compare this value with a value it has generated in the same manner. This comparison is not the same thing as comparing two different bilinear mappings as is required by each of the first and second checks of claim 8. Thus Gentry does not anticipate claim 8.

In rejecting claim 8, the Examiner referred to paragraphs 0028, 0033, and claims 11, 18, 19 of Gentry:

> **Paragraph 0028** describes forming a MAC of a message using the symmetric key as the key of a keyed hash over the message. The symmetric key may, according to line 5, of paragraph 0034, have been formed using the non-interactive shared secret S_{AB}. But paragraph 0028 certainly does not disclose a check involving comparing two different bilinear mappings.
>
> **Paragraph 0033** describes the Figure 5 embodiment and the only relevant part appears to be step 416 concerning each entity confirming that the

other knows the non-interactive shared secret. Paragraph 0034 describes this in more detail as already explained.
Claim 11 is directed to the process by which each entity confirms that the other entity knows the non-interactive shared secret and adds nothing over paragraph 0034.
Claims 18 and 19 make no mention at all of bilinear mappings.

The cited passages do not anticipate claim 8.

Claims 22 and 28

For reasons similar to those discussed above relative to claim 8, independent claims 22 and 28 are not anticipated by Gentry.

Specification amendment

Paragraph 0003 of the description has been amended by this response to address some readily apparent editorial errors.

Claims 18 and 26

The non-elected claims 18 and 26 are cancelled by this amendment without prejudice, and, upon the entry of this amendment, this application should be in condition for allowance.

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2125.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

June 22, 2007
(Date of Transmission)

Mary Ngo
(Name of Person Transmitting)

Mary Ngo
(Signature)

June 22, 2007
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile